FINAL DRAFT

WINDOWS 2003/XP/2000

ADDENDUM

Version 5, Release 0.3

12 July 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

SUMMARY OF CHANGES

July 2005

This document is a compilation of the requirements previously defined in the DISA FSO Windows NT/2000/XP Addendum and DISA FSO Windows 2003 Addendum. Windows NT is no longer supported by Microsoft and has been removed.

The sum total of Windows security requirements is relatively unchanged. However, some requirements have been removed from this document because they are stated elsewhere, either in Microsoft documents or in NSA documents. The remaining requirements are those that are exceptions or additions to the Microsoft and/or NSA security requirements, and are generally here due to DOD policy, or agreements with DOD site customers.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This Addendum to Microsoft's Windows 2003 Security Guide and NSA's Guides to Securing Windows 2000 and XP was developed to enhance the confidentiality, integrity, and availability of sensitive Department of Defense (DOD) Automated Information Systems (AISs) using the Windows 2003, 2000, and XP operating systems (OSs).

This Addendum is coordinated with the following documents here after collectively known as the Windows Server 2003/XP/2000 Guides:

- Microsoft "Solutions for Security, Windows 2003 Security Guide," 2003
- Microsoft "Solutions for Security, Threats and Countermeasures: Security Settings in Windows 2003 and Windows XP," 2003
- Microsoft Windows 2003 and XP Specialized Security – Limited Functionality Templates
- NSA Guide to Securing Windows 2000 Active Directory, December 2000, Version 1.0
- NSA Guide to Securing Windows 2000 Group Policy, September 2001, Version 1.1
- NSA Guide to Securing Windows 2000 Group Policy: Security Configuration Tool Set, December 2002, Version 1.2
- NSA Guide to Securing Windows 2000 File and Disk Resources, 19 April 2001, Version 1.0
- NSA Guide to Securing Windows XP, December 2003, Version 1.1

The Microsoft Windows 2003 and XP Specialized Security – Limited Functionality Templates were developed through the combined efforts of Microsoft, NSA, NIST, DISA FSO, CIS, and other organizations (hereafter referred to as the Consensus Group). They provide a common set of security settings for organizations requiring a highly secure processing environment, such as found in DOD.

Each site network/communications infrastructure must provide secure, available, and reliable data for all customers, especially the warfighter. This Addendum is designed to supplement the security guidance provided by the Windows Server 2003/XP/2000 Guides with DOD-specific requirements. This Addendum will assist sites in meeting the minimum requirements; standards, controls, and options that must be in place for secure network operations. These minimum-security requirements include compliance with the Windows Server 2003/XP/2000 Guides using the Specialized Security – Limited Functionality Templates and the additional requirements defined in this Addendum. Deviations or exceptions will be documented in the appropriate checklist.

It should be noted that FSO support for this Addendum, Checklists, and Tools is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

The requirements set forth in this document will assist System Administrators (SAs), Information Assurance Managers (IAMs), and Information Assurance Officers (IAOs), in securing the Windows 2003, 2000, and XP operating systems for each site. The document will also assist in identifying external security exposures created when the site is connected to at least one Information System (IS) outside the site's control. The site's Configuration Control Board (CCB) will approve all major revisions to site systems.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. SECURITY ADMINISTRATION

This section addresses administrative security requirements that are unique to DOD organizations and are required by DOD directives. However, the concepts outlined here are recommended to any organization requiring a framework for managing security initiatives.

2.1 Security Controls

Windows 2003, Windows XP, and Windows 2000 are operating systems in which the typical OS function and networking are integrated. It provides many configurable security features to secure both the operating system and networking functions. System-level integrity consists of protecting both hardware and software resources. The IAO will ensure a Windows 2003 server, Windows 2000 system, and Windows XP workstation are configured to provide compliance with the security required by *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, Department of Defense (DOD) Directive 8500.1, DOD Instruction 8500.2,* and *OMB Circular A-130*. Use the following guidelines in the acquisition and implementation of products to ensure that security-related issues are adequately addressed:

- *(1.024: CAT II) The SA, under the direction of the IAO, will be responsible for creating, checking, and maintaining a current system baseline for all servers and critical workstations. The IAO is responsible for verifying the system baseline. The IAM will be responsible for setting overall policy for system baseline creation and maintenance.*

- *(1.024: CAT II) The IAM will ensure that sites use a baseline control tool on all servers and critical systems for which the tool is available. This does not apply to special purpose systems where it would degrade the security posture of the system. Examples are firewalls and Cross Domain Solutions (CDS) secure guards that have a minimal Operating System (OS) tailored to the specific requirements of the device.*

A baseline is an image, record, or backup that contains a snapshot of the system after it has been fully loaded with operating system files, applications, and users. Baseline control consists of comparing a current system snapshot with the original system snapshot. The purpose of maintaining and checking a system baseline is to detect unauthorized, undocumented system changes. Unauthorized changes may indicate system compromise and, if detected, could prevent serious damage. A baseline consists of files that change infrequently in terms of size, access permissions, modification times, checksums, or comparable file properties. The SA should maintain three weeks of baseline product reports and be able to provide them upon request. The SA should ensure that all baseline backups are maintained on write-protected media.

- *(1.024: CAT II) The SA will ensure that Baseline reviews are done weekly on each critical system.*

A quick way to perform a baseline review is to create a text file using the dir command. To create the initial baseline file, at the command prompt, enter **dir /s /q %systemroot%*.* >baseline.txt**. This will send the directory contents, including all files, to the file baseline.txt on the C: drive. Be sure to enter a space between ***.*** and the greater than sign (>). After changes have been made, run the same command, but change the filename (baseline2.txt).

To compare the two files, open the new file (baseline2.txt) in MS Word, and perform a file comparison. In MS Word 2000, this can be found on the menu under Tools-Track Changes-Compare Documents. Any file changes will be reflected. The File Compare command can also be used to highlight differences.

Here are two short scripts that can be used to automate the process:

File One:
Baseline.bat (run once per week at the beginning of the week)

echo %date% %time% >baseline.dat
dir /s /q %systemroot%*.* >>baseline.dat

File Two:
Compare.bat (run once per week at the end of the week)

```
echo %date% %time% >baseline2.dat
dir /s /q %systemroot%\*.* >>baseline2.dat
fc baseline.dat baseline2.dat >compare.dat
start /wait notepad compare.dat
del baseline.dat /q
del baseline2.dat /q
```

- *(1.024: CAT II) The SA will ensure that at a minimum, the operating system ***.exe**, ***.bat**, ***.com**, ***.cmd**, and ***.dll** files are baselined and compared.*

- *(1.025: CAT II) The IAM will ensure host-based Intrusion Detection Systems (IDSs) are used on all servers.*

***NOTE*:** Intrusion detection will be provided at the system level. In many situations, full intrusion detection at the enclave level may not be possible due to VPN or application layer encryption.

2.2 Open Source Software

DOD has clarified policy on the use of open source software to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. DOD no longer requires that operating system software be obtained through a valid vendor channel and have a formal support path, if the source code for the operating system is publicly available for review.

DOD CIO Memo, "Open Source Software (OSS) in Department of Defense (DOD), 28 May 2003:

- "DOD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DOD policies that govern Commercial-Off-The-Shelf (COTS) and Government-Off-The Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DOD information systems whether acquired of originated within DOD;

- Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and;

- Be configured in accordance with DOD-approved security and configuration guidelines at http://iase.disa.mil/ and http://www.nsa.gov/."

Open source software takes several forms:

1. A utility that has publicly available source code is acceptable.

2. A commercial product that incorporates open source software is acceptable because the commercial vendor provides a warranty.

3. Vendor supported open source software is acceptable.

4. A utility that comes compiled and has no warranty is not acceptable.

2.3 Patch Control

Maintaining the security of a Windows Server 2003/XP/2000 system requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch (hot fix) to overcome security vulnerabilities.

SAs and IAOs should regularly check OS vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

- *(1.029: CAT III) The IAO and SA will subscribe to the DOD JTF-GNO/VCTS (Vulnerability Compliance Tracking System) bulletin mailing list.*

- *(2.019: CAT II) The IAO will ensure that all security-related software patches are applied and documented.*

- *(2.005: CAT II) The IAO will ensure that the latest OS and Application service packs are applied and documented.*

NOTE: Generally a couple of months will be allowed for any problems to be reported to the vendor prior to new service packs being required.

2.3.1 DOD Patch Repository

DISA maintains a repository of software patches and hot fixes.

This patch server can be accessed at the following location:

NIPRNet - https://patches.csd.disa.mil

2.3.2 Microsoft Software Update Services (SUS)

SUS is Microsoft's Solution for distributing and installing Windows critical updates and Windows security roll-up patches using the Automatic Updates feature on a Windows client and the Background Intelligent Transfer Service (BITS). Windows XP SP2 has BITS 2.0 included. Windows XP SP1 can be upgraded with BITS 2.0.

Organizations that utilize SUS have options for implementation. A local SUS server can be configured to pull updates from either Microsoft or another SUS server (such as a DOD SUS server). The existence of a DOD SUS server eliminates security issues for obtaining patches, and prevents users from downloading and applying patches that the site has not approved. Each client machine using the Software Update Services is configured to pull updates from another server running SUS. The configuration of the client allows SAs to set certain parameters for the install such as user notification that updates are available as well as the timing and notification that a reboot will occur.

The administrator of the local SUS server has configuration options that can control the deployment of each patch or allow SUS to be configured to deploy the patches as soon as they are received. This gives the flexibility to either test before deployment or have the patches immediately available for deployment.

For a client to be able to utilize an authorized SUS Server the following must be configured:

- The Automatic Updates, and Background Intelligent Transfer Service (BITS) services must be active.

The following options must be configured in the Local Security Policy (or Group Policy):

- Using the Local Security Policy snap-in in the Microsoft Management Console (MMC), expand Computer Configuration/Administrative Templates.
- Right click Administrative Templates and select “Add/remove templates.”
- Select “Add”; then select %systemroot%\Inf\WUAU.ADM, and select “Open.”
- Select “Close.”
- Expand Administrative Templates\Windows Components\Windows Updates.
- Select and enable “Configure Automatic Updates.”
- Select and enable “Specify intranet Microsoft update service location.” Enter the appropriate web site into both server fields. (“Set the intranet update server for detecting updates” and “Set the intranet statistics server.”)
- Select “Close.”
- Exit from the MMC.

The DOD SUS server is located at the following:

NIPRNet – http://dodsus.csd.disa.mil

This page is intentionally left blank.

3. SECURING THE WINDOWS 2003/XP/2000 OPERATING SYSTEM

3.1 Permitted Operating Systems

Windows 2000 has been NIAP approved, and Windows 2003 and Windows XP are currently undergoing NIAP Certification.

- *(5.003: CAT II) The IAO will ensure that the system boots only to STIG compliant operating systems.*

- *(2.005: CAT II) The IAO and SA will ensure that the Windows OS, at a minimum, has had the latest service pack installed.*

- *(3.002: CAT II) The IAO and SA will ensure that configuration settings and files that support the Posix operating system are removed from the machine, unless there is a documented requirement for this support.*

- *(2.020: CAT I) The IAO and SA will ensure unsupported system software is removed or upgraded prior to a vendor dropping support.*

- *(2.020: CAT II) The IAO will ensure that the site has a formal migration plan for removing or upgrading OS systems prior to the date the vendor drops security patch support.*

This page is intentionally left blank.

4. SECURING THE REGISTRY AND WINDOWS 2003/XP/2000 POLICIES

4.1 Windows 2003/XP/2000 Registry Access Policy

Implementing security measures within the Windows 2003/XP/2000 environment includes using the Registry Editor. Incorrect use of the Registry Editor can cause serious system-wide problems that may require the reinstallation of the Windows operating system to correct them. Microsoft does not guarantee that any problems resulting from the use of the Registry Editor can be solved and warns to use this tool at one's own risk. Only a highly trained SA should modify registry settings.

- *(1.006: CAT II) The IAO will ensure that only trained, authorized SAs can access the registry to perform the Registry Editor function.*

NOTE: A system backup, to include system state data, should be created before any changes and retained for at least five working days after the changes. After changes have been completed and a successful reboot has been accomplished, an "after changes" backup should be made and maintained. If possible, a current backup that includes system state data should be available for all critical servers.

4.2 Active Directory/Group Policy Access Policy (Windows 2003/2000)

Most security measures in Windows 2003/XP/2000 are implemented using Group Policies that reside in the Active Directory. Group Policy can affect every machine in the network. Incorrect use of Group Policy could in theory bring down an entire network or cause a denial of service across an entire network. It is essential that the Active Directory and Group-level policies be protected from unauthorized or untrained persons making alterations to them.

- *(1.006: CAT II) The IAO will ensure that only trained, authorized SAs can access the Active Directory and Group-level policies for the purpose of adding policies or performing maintenance.*

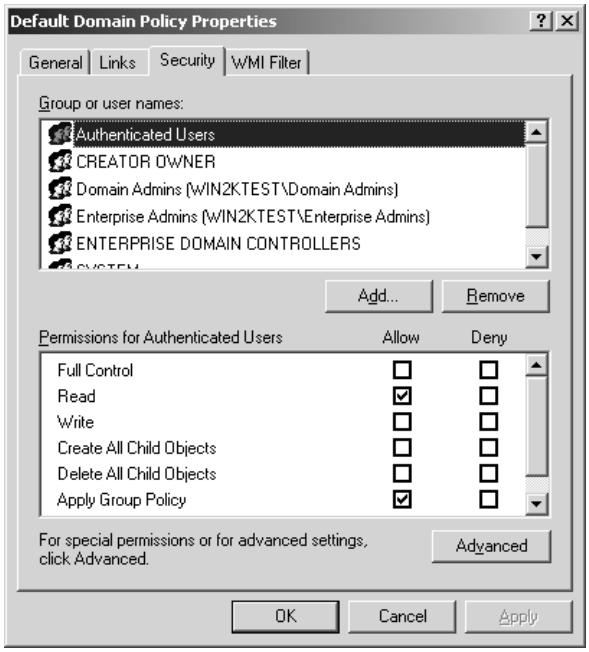
- *(2.013: CAT I) The IAO will ensure that security recommendations for "Group Policy" and "Active Directory" in the Microsoft Server 2003 Guides are enforced.*

4.2.1 Group Policy Permissions (Windows 2003/2000)

Access permissions need to be applied properly to Group Policy Objects to protect them from unauthorized access and unwanted modification. Permissions should be set for all Group Policies that may be assigned at the site, domain, or organizational unit level. The procedure for setting permissions is basically the same, regardless of the level at which it is assigned.

The Group Policy is accessed through the following procedure.

Select Start -> Programs -> Administrative Tools.
Select Active Directory Users and Computers (for Domain and OU policies).
--Or--
Active Directory Sites and Services (for Site policies).
Select the Domain, OU, or Site name in the left-hand window.
Right-click on the selected name.
Select Properties.
Select the Group Policy tab.
Click on Properties.
Select the Security tab.



Users should be restricted to "Read" and "Apply Group Policy." Only *Administrator-related* groups, Creator Owner, or System can have less restrictive privileges.

The site can define more restrictive permissions by building groups that contain the specific administrators responsible for maintaining group policies and removing the more inclusive Administrator groups. Administrator responsibilities can be divided through the use of Organizational Units to more accurately reflect a division of duties. Administrators can be limited to modifying Group Policy only for the Organizational Unit for which they are responsible. This limits the scope of damage should one administrator make an accidental or malicious change that would adversely affect the network.

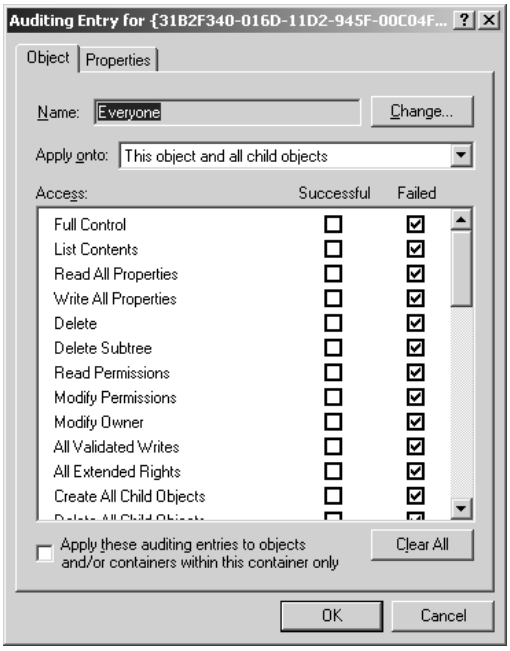
- *(2.013: CAT I) The IAO will ensure that ACLs for Group Policies restrict access to only authorized accounts.*

4.2.2 Group Policy Object Auditing

The integrity of Group Policy Objects is essential for protecting all the computers assigned to the Forest and associated Domains. Auditing should be configured on each Group Policy Object and event logs should be reviewed for failed access attempts.

Group Policy audit options are accessed through the following procedure.

Select Start -> Programs -> Administrative Tools.
Select Active Directory Users and Computers (for Domain and OU policies).
--Or--
Active Directory Sites and Services (for Site policies).
Select the Domain, OU, or Site name in the left-hand window.
Right-click on the selected name.
Select Properties.
Select the Group Policy tab.
Click on Properties.
Select the Security tab.
Click the "Advanced" button and select the Auditing tab.
Click the "Add" button and enter "Everyone".
On the Object Tab of the Auditing Entry screen check failed option for "full control."
Click "OK," "OK," "OK."



- *(2.021: CAT II) The IAO will ensure that auditing related to Group Policy and Active Directory is properly configured.*

4.3 Registry Settings

The following security settings are made directly in the Registry using the **regedit.exe** editing program. On Windows 2003/XP/2000 systems, provision has been made to modify some of these settings through the MMC, using Security Configuration and Analysis, and Policy snap-ins. Follow the general guidance for modifying Security Options in the Windows 2003/XP/2000 guides. Explicit instructions for systems, when applicable, are provided in the following sections.

The following sections outline recommended additions to the registry changes required by the *Windows 2003 Guide* and the *NSA XP and 2000 Guides.*

NOTE: On Windows 2003/XP/2000 machines, load the updated Security Options File, following instructions in *Section 5.1* in the Checklists. This file adds additional Consensus Group security configuration options to the Configuration and Analysis and Policy plug-ins.

4.4 Recommended Settings Variations

4.4.1 LMCompatibilityLevel Registry Key

Procedures for configuring the LMCompatibilityLevel Registry key for Windows 2003 are listed in the *Microsoft Windows 2003 Security Threats and Countermeasures guide*, and for Windows XP and 2000 are listed in the *NSA XP and 2000 Guides*.

NOTE: In a mixed-mode Windows 2000 or 2003 environment, the required setting (send NTLMv2 only) for the LMCompatibilityLevel Registry key may cause authentication failures, and trust failures while trying to map shared resources in another domain. It is recommended to set the Registry key value to 2, if this problem occurs.

- *(3.031: CAT II) The SA will ensure that the LMCompatibilityLevel registry key is set to the highest level that will work in his environment. At a minimum, this key must be set to at least **2**. A value of **0** or no key is not acceptable.*

Example:

Using the MMC Local Policy snap-in:

In the left-hand tree window, select Security Settings -> Local Policies -> Security Options.

In the right policy window, select the “Network Security: LAN Manager authentication level” option and set it to “Send NTLMv2 response only\refuse LM & NTLM.”

NOTE 1: In NT domains, set it to "Send NTLM response only." In a Windows 2000/2003 domain running **Exchange**, this setting may need to be set to not exceed level 4 "Send NTLMv2 response/refuse LM," on Domain Controllers and the Exchange Server.

NOTE 2: This option can also be configured using the Security Configuration and Analysis snap-in, or for multiple machines with the Group Policy snap-in.

4.4.2 Password Policy

The requirements below are exceptions and additions to the Password Policy recommended by the Microsoft Server 2003 Security Guides and the NSA Windows 2000 and XP Guides.

- *(2.009: CAT II) The SA will ensure that the complex password filter, EnPasFlt.dll, which was developed by NSA, or Password Policy Enforcer (PPE), is installed and active on each machine, and that each password is composed of at least one of each of the four character types: upper case, lower-case, numeric, and special characters.*

NOTE 1: For the EnpasFlt external password filter to be effective, the Password Policy option "Password must meet complexity requirements" must be disabled. However, if an external password filter is not used, then it should be set to enabled to ensure a minimum level of password complexity. If password complexity is turned on, then this finding can be downgraded from a Category II to a Category IV.

NOTE 2: Under Windows 2003/XP/2000, several user accounts may generate false findings in an Security Readiness review (SRR), saying that the account is not required to have a password. (i.e., Guest, IUSR_…, TSUser). The SA can correct this problem by entering the following on a command line:

Net user <*account_name*> /passwordreq:yes

User account Passwords must be changed at least every 90 days, and will expire after that period. However, this is not a reasonable setting for accounts that are used solely by applications. Generally, if an application account password expires, the application will cease to function. Application Accounts can be configured to not expire.

- *(4.018: CAT II) For Application accounts, the IAM will ensure that there is a local policy in place that requires passwords to be changed on a yearly basis.*

NOTE: For applications that internally generate complex passwords, or where changing the password would require an unreasonable effort or endanger the availability of a critical application, this is not required (e.g., IUSR_xxx).

4.4.3 Caching of Logon Credentials

Windows 2003/XP/2000 will cache the credentials of users who log on interactively. In the event that a domain controller is unavailable for processing a logon, the stored credentials will permit a user to log on. This can pose a security risk if an intruder gets physical access to the machine and can get the cached credentials. To mitigate this risk the number of logon credentials stored should be limited to two or less.

Example:

Configure or delete the following security option:

"Interactive Logon: Number of previous logons to cache (in case Domain Controller is not available)" should be set to "2 logons" or less.

- *(30.013: CAT III) The SA will ensure that a number of previous logons to cache is set to 2 or less.*

5. USER RIGHTS

The recommendations specified in the Windows Server 2003/XP/2000 Guides will be followed in assigning user rights. In addition, the SA will ensure that the following requirements are applied:

The right to act as part of the operating system can potentially permit an account to bypass the security features of Windows. Therefore it is a serious security vulnerability to grant this right to any individual or group. However, some applications require this and other restricted rights to function properly. Passwords for these accounts will be the maximum length permitted, will follow the strong password rules, and will be kept in a locked container accessible only by the IAO and his or her designated backup. In this situation, these restricted rights may be permitted under the following conditions:

- *(4.009: CAT I) The IAO will ensure accounts receiving the right Act as Part of the Operating System are clearly identified and documented.*

Exceptions may be made to the recommended setting for applications that require specific rights to function properly. Vendor installation documentation will generally specify what those rights are. Generally, the rights are only required on the box on which the application is installed. Exceptions are only permissible for an application account, which is one that the application uses internally, and is never used by an individual user to log on.

- *(4.010: CAT II) The IAO will ensure that exceptions to User Rights recommendations for applications are documented.*

This page is intentionally left blank.

6. AUDITING

6.1 Audit Log Management

6.1.1 Evaluating Audit Trails and Log Files

Auditing will be enabled and configured in accordance with the guidelines in the *Windows 2003 Guides, NSA XP and 2000 Guides,* and *Section 6, Auditing*, of this document. To be of value, audit logs from servers and other critical systems will be reviewed on a daily basis to identify security breaches and potential weaknesses in the security structure.

- *(1.029: CAT II) The IAO will have local policies for archiving, reviewing, and evaluating audit trails.*

6.1.2 Protecting Logs

The Event Log entries in Windows 2003/XP/2000 can be critical in providing information relating to unauthorized access to the system. To be useful as evidence in any judicial proceeding, the information in these logs must be protected and access limited to only those individuals whose job it is to evaluate and maintain these files.

File access restrictions can be set to limit the clearing and editing of the Event Logs to authorized members of an Auditors group. However, because of the structure of Windows, members of the Administrators group will still be able to view and edit the logs, if they use their privileges to modify their user rights. Therefore, local policies will preclude administrators, as a group, from changing those rights and ensure that only members of the Auditors group will be authorized change access to the Event Logs.

NOTE: The administrator(s) responsible for the installation and maintenance of the individual system(s) must be a member(s) of the Auditors group. This will permit the responsible administrator to enable and configure system auditing, and perform maintenance functions related to the logs. Administrators who are not responsible for maintenance on an individual system will not be included in the Auditors group.

- *(1.010: CAT II) The IAO will protect Event Logs from unauthorized administrators or users who might change or delete them. All access to Event Logs will be audited, and archived logs will remain under locked control.*

- *(1.010: CAT II) The IAM will ensure Local policy precludes those accounts, which are not part of the Auditors group, from changing the file access restrictions on Windows Event Logs.*

- *(2.001: CAT II) The IAO or SA will ensure Full Control access to the Event Logs is given to an Auditors group. The Auditors group contains those individuals who are authorized to archive and clear the log.* (The Administrators group can be given *read* access.)

NOTE: Under Windows, when an event log is cleared, the system deletes and recreates the log file. This, in effect, restores the default file permissions to those of the parent directory. Permissions for the "Auditors" group are removed and the Administrators group receives full control. To prevent the problem of having to reset permissions on the event log whenever it is cleared, use the following optional procedure:

1. Create the following directory: %SystemRoot%\system32\config\EventLogs.
2. Set ACL permissions on this directory. (Auditors – Full Control, System – Full Control, Administrators – Read)
3. Copy the event logs from the \config directory to the new EventLogs directory.
4. Edit the Registry using regedit.exe.
5. Expand the following key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog.
6. Select the Application key.
7. Double-click the "File" value.
8. Change the string value to: %SystemRoot%\system32\config\EventLogs\Appevent.evt.
9. Repeat Steps 5 through 7 for "Security (Secevent.evt)" and "System (Sysevent.evt)."
10. The next time the machine is rebooted it will use the event logs in the EventLogs directory.
11. After reboot, remove the old event logs from the \config directory.

6.2 Audit Log Requirements

Auditing is a key component in maintaining a secure computing environment. The scope of the auditing effort should be carefully planned to be consistent with operational requirements and system responsiveness. The number of machines supported may prevent a SA from implementing and managing a viable auditing effort. Every effort should be made to implement auditing according to the *Windows 2003 Guides, and NSA XP and 2000 Guides* and this document.

Log size can be reduced if the site has an alternative auditing methodology that ensures the longevity and integrity of the data. The number of days before Event Log Wrapping occurs should be set to seven days to preserve data if a problem occurs with the alternative methodology. The Audit Server project implemented by FSO is an acceptable solution.

Microsoft recommends that the combined sizes of all event logs should not exceed 300 megabytes. On servers this total should include any DNS and Directory Services logs. This limitation is due to the way all Windows systems handle the logs in memory. Exceeding this limit could impact system performance.

- *(5.001: CAT II) The SA will ensure Event Log Wrapping is set to "Do not overwrite Events" (Clear log manually) for Windows 2003/2000 servers. For Windows XP and Windows 2000 Professional this can be configured to overwrite after 14 days.*

6.3 Audit Failure Procedures

A site will have a documented procedure in place to identify, in a timely manner, that critical systems have stopped writing to the event logs. The procedure will include instructions for

protecting and archiving log data. If a site does not have a documented procedure, then all servers and machines that a site deems critical will be configured to halt processing if an audit failure occurs.

With Windows 2000 SP3, Microsoft introduced the ability to automatically archive and clear an event log when it becomes full. This procedure works whether the setting for halting the system if the log becomes full, is on or off. The following procedure can be used to turn on this archive function:

1. Edit the Registry using regedt32.exe.
2. Expand the following key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog.
3. Select the appropriate event log key (e.g., Security, Application, System, etc.).
4. Select Edit -> Add Value from the Menu Bar.
5. Type "AutoBackupLogFiles" in the Value Name field, and select "REG_DWORD" in the Data Type drop-down box. Click "OK."
6. Type a "1" in the Data field on the Dword Editor box that appears. Click "OK."
7. Repeat Steps 3 through 6 for each event log.

The automatic archive process will create the archived log file in the %SystemRoot%\System32\Config directory. It will probably be necessary to move these files to another location on a regular basis to prevent the drive with the system files from filling up. A simple script could be written to accomplish this.

For more information on this automatic backup behavior, see Microsoft TechNet article Q312571 at http://support.microsoft.com/default.aspx?scid=kb;en-us;312571.

If a system has been configured to stop processing when an audit failure occurs, the system will crash with a *blue screen*, indicating that a failure event took place. At this point, only an administrator will be able to log on to the box, so that the problem can be resolved and auditing can be restarted.

6.4 Audit Alternate Data Streams (ADS)

An approved commercial tool should be used periodically to check for ADS. ADS is a method for data hiding that hackers may use to store system data that is invisible to the file system.

This page is intentionally left blank.

7. GENERAL SECURITY MEASURES

7.1 File Security

For Windows Server 2003 and Windows XP, NSA has determined that the default Microsoft ACL settings are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" and Power User Group Membership is restricted for all accounts.

The following requirement applies when the conditions above are not met, and for all Windows 2000 systems:

- File permissions will be configured to meet the recommendations in *Appendix A* of this document. Separate partitions should be created to house application files. File and directory ACLs on application partitions should be changed from the system defaults and give users only the minimum permissions required for applications to function efficiently. The Everyone group will be replaced with the Users group.

- Any file share permissions should also be changed from the default, by removing the "Everyone" group and replacing it with the "Users" group, or by defining more restrictive explicit permissions.

- *(2.015: CAT II) The SA will ensure that the "Everyone" group is replaced on ACLs for file shares.*

- *(2.015: CAT II) The SA will ensure that, on Application Servers, regular users do not have write or delete permissions to shares containing application binary files (i.e., .exe, .dll, .cmd, etc.).*

7.1.1 Mobile USB Disk Devices

Mobile USB Disk devices are designed to plug into the USB port on a Windows 2003/XP/2000 machine. If the Plug and Play service is running, and the USB ports are not disabled, then the device is recognized and installed without intervention, and will appear as another removable drive in Windows Explorer.

These devices are small and portable and can be easily stolen. Physical protection of the device is essential.

These devices are also easily concealable. Generally, Windows will immediately recognize that the USB device has been connected, and will activate it. An unauthorized individual could quickly attach the device, copy sensitive files, and disconnect it in a short period of time.

If sensitive information is stored on a USB device, it should be encrypted using an encryption routine that meets DOD encryption standards. The Windows Encrypted File System or third party product can be used to encrypt files.

A user can set permissions for the files stored on the device, and also enable the system to audit any unauthorized access, by configuring the device using the Windows NTFS file system. They can be formatted and configured from the command line using the format:

<USB drive letter> /FS:NTFS

After formatting, clean-up user access to the USB drive by:

- If the Server is on a domain, remove all built-in accounts, remove the everyone group, and add the domain user authorized to access the data. If the domain controller is down, there are connectivity issues, or if the user is attempting to log on locally, and there are no cached credentials the user will be unable to use the USB drive.

- If the Server is not on a domain, remove the everyone group and add the user or user type to the device.

Permitted devices should be restricted to those purchased by the government. Each device should be physically marked with the appropriate classification label. It should also be protected, transported, and disposed on in accordance with the DOD regulations appropriate to the data stored on it.

When using to move data from USB drive to unclassified or classified systems such as loading scripts or other tools, only write protected USB drive devices will be used. Write protect will be invoked. When this procedure is followed, the device cannot be written to and therefore, does not become classified.

- *(2.017: CAT II) The IAO will ensure that sites have a clearly defined local policy on the use of Mobile USB Disk devices.*

- *(2.017: CAT II) The IAO will ensure that sensitive data on Mobile USB Disk Devices are protected with a DOD approved encryption scheme.*

7.2 Network Printers

Printers that are shared on the network should be configured to restrict their use to authorized users. Permissions should be reconfigured to be more restrictive than the defaults assigned when the share is created. The table below shows the minimum permissions required:

Settings	
Users:	Print
Administrators:	Full Control
SYSTEM:	Full Control
CREATOR OWNER:	Full Control

- *(3.027: CAT III) The SA will ensure that print share permissions are configured according to requirements.*

7.3 Logging Off or Locking the Server/Workstation

Users should either log off or lock the server if they will be away from the computer for any length of time.

Logging off allows other users to log on (if they know the password to an account); locking the session does not. If a server is not used for a set period of time, the server can be set to lock automatically by using any 32-bit screen saver with the Password Protected option.

- *(5.006: CAT II) The SA will ensure systems are configured to automatically lock with a password-protected screen saver after inactivity of no more than 15 minutes. Five minutes is recommended.*

Applications requiring continuous, real-time screen display (i.e., network management products) will be exempt from the inactivity requirement provided the following requirements are met:

- The logon session does not have Administrator rights.
- The inactivity exemption is justified and documented by the IAO.
- The display station (i.e., keyboard, CRT) is located in a controlled access area.

7.3.1 Configuring Default User Screensaver Options

In an environment where roaming profiles are not used, every user logging on to a Windows 2003 machine for the first time has a profile built using the default user profile stored in the %Systemdrive%\Documents and Settings directory. The default profile can be configured to apply the password-protected screen saver requirements.

- *(3.006: CAT II) The SA will ensure the default user screensaver options are configured to conform to DOD requirements.*

The default user profile is a registry hive, and as such, it can be edited with the following procedure:

1. Start Regedit. When it opens, select the Hkey_Users root key.

2. On the menu bar, select the Registry>Load Hive option to select the default user profile to be edited. It is located in the %Systemdrive%\Documents and Settings\Default User directory as Ntuser.dat.

3. When Regedit asks for a key name, give it a name the user recognizes. Regedit will import the hive and attach it under the root key under the *hive name* specified.

4. Select the new hive key, right click on it, and select Permissions menu item to add Users: Read access to the key and its subkeys. This enables the profile sharing mechanism to copy keys from the default profile to users' Hkey_Current_Users.

5. Use Regedit to make the recommended STIG changes to subkeys of the new hive. As changes are made, the hive file will be updated. Set the following values on the *hive name* \ControlPanel\Desktop key:

   - ScreenSaveActive : REG_SZ : 1
   - ScreenSaverIsSecure : REG_SZ : 1
   - ScreenSaveTimeout : REG_SZ : 900 (*in seconds, 900=15 minutes*)
   - SCRNSAVE.EXE : REG_SZ : logon.scr

6. Once all the hive keys are edited, use the Registry>Unload hive menu item to detach the hive. These settings will now be applied to a new profile when it is created.

NOTE: Use this same procedure to configure profiles that already exist on a Windows machine so that they comply with security requirements.

7.4 Installed Services

Windows 2003/XP Services typically run under two new service accounts, the Network Service and Local Service, which generally restrict permissions that are required by the service. Compromising a service could allow an intruder to obtain System permissions and open the system to a variety of attacks. The Local Service account has complete privileges on the local system. The Network Service has limited privileges on the local system. Windows 2000 Services generally run under the local System account.

When possible, the SA will configure services to run under local accounts with the minimum permissions and rights needed to perform their task.

- *(2.014: CAT II) The SA will restrict access to disabled services by configuring the following ACL permissions on each service object: Administrators, "Full Control," "System" "Full control," and Authenticated Users "Read."*

- *(3.061: CAT I) If services are to be accessed remotely (e.g., file transfer protocol (FTP)), the IAO will ensure that a secure shell product is used to encrypt the userid and password.*

NOTE: Encryption of the user data inside the network firewall is also highly recommended. Encryption of user data coming from or going outside the network firewall is required. Encryption for Administrator data is always required. Refer to the *Enclave Security STIG* section on "FTP and Telnet," for detailed information on their use.

The Windows 2003 and XP Specialized Security – Limited Functionality Templates, developed by Microsoft and the Consensus Group, recommends a list of services that should be disabled. Sites should disable the services on these lists, unless there is a real requirement for specific

services. Required services will vary between organizations. Organizations will develop their own list of services that are exceptions to the recommended disabled list, and any additional services that are not specified by Microsoft. Exceptions will be documented and justified with the IAO. This list will be provided for any security review. Services that are common to all systems can be addressed in one document. Exceptions for individual systems should be identified separately by system.

- *(5.068: CAT II) The IAO and SA will ensure that unnecessary services are removed or disabled.*

7.5 Virus Protection

Malicious programs that result in a denial of service or corruption of data can be thwarted with scanning programs that look for signatures of known viruses. Several virus scanning and cleaning products are available for free download from the DOD JTF-GNO web page. Some of the packages on the server are McAfee's AntiVirus and Symantec (Norton) Antivirus. These are governed by a DOD site license. The address for downloading is http://www.cert.mil (NIPRNet).

The *Desktop Application STIG* provides complete requirements for anti-virus software. Configure the product using that guidance.

- *(5.007: CAT I) The SA will ensure an approved anti-virus product is installed and enabled, and ensure signature files are no older than 14 days. (In the event that a signature file is not released by JTF-GNO in the last 14-day period, then the most current release is required.)*

NOTE: Some corporate firewall products, such as Raptor, are incompatible with antivirus software. On these boxes, this requirement does not apply. Personal firewall products, however, are not exempt.

- *(5.007: CAT I) The SA will ensure signature files will be no older than 14 days. (In the event that a signature file is not released by JTF-GNO in the last 14-day period, then the most current release is required.)*

The use of products by DOD organizations, other than those available on the DOD JTF-GNO web site, is discouraged. DOD has special licensing agreements with both McAfee and Symantec.

Some vendors of virus protection software make beta versions of their signature files available to their customers. These have not been tested, and should not be downloaded and used.

7.6 DCOM

Microsoft's distributed COM (DCOM) extends the Component Object Model (COM) to support communication among objects on different computers—on a LAN, a WAN, or even the Internet. With DCOM, an application can be distributed at locations that make the most sense to the user and to the application.

7.6.1 Distributed Component Object Model (DCOM)

DCOM achieves security transparency by letting developers and administrators configure the security settings for each component. Just as the NTFS lets administrators set access control lists (ACLs) for files and directories, DCOM stores Access Control Lists for components. These lists simply indicate which users or groups of users have the right to access a component of a certain class. These lists can easily be configured using the DCOM configuration tool (DCOMCNFG) or programmatically using the Windows 2003/XP/2000 Registry and Win32® security functions.

- *(5.107: CAT II) The SA will ensure the default DCOM authentication level is set at **connect** or above.*

- *(5.109: CAT II) The SA will ensure that the default DCOM access permissions are configured to prevent non-administrators from creating DCOM objects and executing code on the local system.*
  (Recommended: Administrators, Interactive Users – Allow Access)

- *(5.110: CAT II) The SA will ensure that the default DCOM launch permissions are configured to prevent unauthorized users from launching applications.*
  (Recommended: Administrators, Interactive Users – Allow Launch)

- *(5.106: CAT II) The SA will ensure access permissions on DCOM objects do not permit non-administrators to create DCOM objects and execute code on the local system.*

- *(5.111: CAT II) The SA will ensure launch permissions on DCOM objects do not permit unauthorized users to launch applications.*

- *(5.108: CAT II) The SA will ensure that the Registry Keys for DCOM objects have ACLs to prevent non-administrators from changing security settings.*
  (Recommended: Administrators, Creator Owner, System – Full, Users – Read)

DCOMCNFG.EXE is in the %systemroot%\System32 directory. It can be used to set access security on DCOM objects and specify the authorization level.

7.6.2 Altered DCOM RunAs Value

DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. If present, the RunAs value tells the COM Service Control Manager (SCM) the name of the account under which the server is to be activated. In addition to the account name, the COM SCM must also have the password of the account. The result of a successful logon is a security context (token) for the named account that is used as the primary token for the new COM server process. Administrators should not use this method in the evaluated configuration if accountability is required, since accountability cannot be enforced. RunAs values will be removed.

Remove the following registry value:

Hive: HKLM
Key: \Software\Classes\AppID\
Name: "Each subkey listed"
Value: RunAs

- *(5.112: CAT II) The SA will ensure that DCOM calls are not executed under the security context of a user specified in a RunAs parameter.*

7.7 Recycle Bin (Windows 2003/2000 Server)

The Recycle Bin saves a copy of a file when it is deleted through Windows Explorer. This poses a security risk. A user may delete a sensitive file and yet still leave a copy of that file in the Recycle Bin.

- *(3.051: CAT III) The SA will ensure the Recycle Bin on servers is configured to "remove files immediately when deleted."*

To configure the Recycle Bin to prevent deleted files from being saved, use the following procedure:

- Right click the Recycle Bin icon on the desktop, and select Properties.

- Check the box labeled, "Do not move files to the Recycle Bin. Remove files immediately when deleted."

- Click "OK."

- Empty the Recycle Bin of any pre-existing files.

Another security risk associated with the Recycle Bin is the %systemdrive%\Recycler directory that does not show all information to the graphical display. Hackers have been known to use the Recycler directory for storage. A user may be locked out to writing to a drive or directory by file permissions, but all users can delete their files to %systemdrive%\Recycler. Periodically check the contents of %systemdrive%\Recycler to look for anomalous entries and delete. Unknown or rogue entries in the %systemdrive%\Recycler folder may be indicative of an intrusion.

8. APPLICATION SECURITY

8.1 Removing Unneeded Applications

Applications that are no longer needed should be removed from the system. Unused applications are generally not updated, or patched, and can provide a means for unauthorized persons to exploit vulnerabilities to gain access to the system. This includes Microsoft applications that may be installed when the operating system is installed.

Unwanted applications should be removed using a vendor provided uninstall function or using the Windows "Add /Remove Programs" applet. It is not sufficient to just delete desktop icons and application directories. The uninstall functions also clean up the application's registry entries.

NOTE: If unwanted applications have not been completely removed using the above procedures, they will still be considered as installed for SRR and IAVM purposes.

8.1.1 Microsoft Zone Internet Games (Windows XP)

The new Internet Games opens a limited connection to the free games section of the MSN Gaming Zone, which is located at www.zone.msn.com. DOD sites should be prevented from accessing these games.

- *(5.021: CAT III) The SA will ensure that the Microsoft Zone Internet Games option is not installed on the system.*

8.1.2 MSN Explorer (Windows XP)

MSN Explorer is automatically installed with Windows XP. MSN Explorer is a feature that connects the user to the free non-subscriber section of the MSN.com Web site. From this default site the user has access to all of the MSN services. The MSN.com Web site is an Internet connectivity service that provides access to a variety of personal-interest information and services, as well as providing a portal to the World Wide Web.

- *(5.022: CAT III) The SA will ensure that MSN Explorer is not installed on the system.*

8.1.3 IIS Components (Windows XP)

Windows XP comes with a version of Internet Information Services (IIS) that can optionally be installed. This feature permits the hosting of a Web site on the Windows XP machine. Web sites should only be hosted on servers that have been designed for that purpose and can be adequately secured.

- *(5.016: CAT I) The IAO will ensure that IIS, or any subset of the Internet Information Services, is not installed on the system.*

8.1.4 .NET Framework

The Microsoft .NET Framework, also referred to as the Common Language Runtime (CLR), provides an operating environment similar to the Java Runtime Engine (JRE). Programs written and compiled to the .NET Platform may be run on any system with a CLR installed, regardless of the underlying OS.

One of the principal goals of the .NET Platform is to provide a common operating environment for web-based applications. .NET mobile code is currently uncategorized. According to the DOD mobile code policy, uncategorized mobile code is not allowed to execute on any DOD system. The .NET Framework may only be used for locally executed applications, that are locally developed or DOD approved, or to support local applications and services that require it.

The .NET Framework includes a complex security model that is currently being evaluated. It can be uninstalled from Windows 2000 and Windows XP, but is integrated into the Windows 2003 operating system.

- *(5.069: CAT II) The IAO will ensure that the .NET Framework is configured to prevent the execution of unauthorized mobile code.*

Microsoft has already released Service Packs for the .NET Framework that fixes several problems. If the .NET Framework is installed, it must be upgraded to the current .NET Framework Service Pack, and include any security related hot fixes.

- *(5.069: CAT II) The IAO will ensure that the .NET Framework, if it is installed, is upgraded to the current Service Pack, and includes any security related hot fixes.*

9. DISASTER RECOVERY

9.1 Active Directory Backups (Windows 2003/2000)

Active Directory is the heart of a Windows 2003/2000 domain. If the Active Directory becomes corrupted, and no backup copy exists, it will probably be necessary to reinstall the entire domain. Therefore, it is essential to maintain a current backup to ensure a timely continuance of operations, should problems occur. SAs should ensure that a current backup of the Active Directory is made prior to making any significant changes.

- *(1.023: CAT II) The Active Directory will be backed up on Server 2003/Windows 2000 domain controllers on a weekly basis.*

This page is intentionally left blank.

APPENDIX A. REQUIRED FILE, FOLDER, AND REGISTRY PERMISSIONS

For Windows Server 2003/XP, NSA has determined that the default ACL settings are adequate when the Security Option "Network access: Let everyone permissions apply to anonymous users" is set to "Disabled" and Power User Group Membership is restricted.

In a Mixed Windows environment (containing systems with Windows NT 4 or WIN9x, /ME) and for all Windows 2000 systems, the following file ACLs will be configured:

File and Folder Permissions:

File and Registry ACL settings are always required for Windows 2000 systems, and are required for Server 2003 and Windows XP when the Power Users Group is not restricted, or Anonymous has not been restricted from the Everyone Group. Otherwise, the Microsoft default ACL settings are sufficient.	
%SystemDrive%	Administrators: Full System: Full Creator Owner: Full Users: Read, Execute. (This should only apply to the directory and not propagate.)
%SystemRoot% \regedit.exe	Administrators: Full System: Full
%SystemRoot% \System32\arp.exe	Administrators: Full System: Full
%SystemRoot% \System32\at.exe	Administrators: Full System: Full
%SystemRoot% \System32\attrib.exe	Administrators: Full System: Full
%SystemRoot% \System32\cacls.exe	Administrators: Full System: Full
%SystemRoot% \System32\debug.exe	Administrators: Full System: Full
%SystemRoot% \System32\edlin.exe	Administrators: Full System: Full
%SystemRoot% \System32\eventcreate.exe	Administrators: Full System: Full
%SystemRoot% \System32\eventtriggers.exe	Administrators: Full System: Full
%SystemRoot% \system32\ftp.exe	Administrators: Full System: Full
%SystemRoot% \System32\nbtstat.exe	Administrators: Full System: Full
%SystemRoot% \system32\net.exe	Administrators: Full System: Full

%SystemRoot% \system32\net1.exe	Administrators: Full System: Full
%SystemRoot% \system32\netsh.exe	Administrators: Full System: Full
%SystemRoot% \System32\netstat.exe	Administrators: Full System: Full
%SystemRoot% \System32\nslookup.exe	Administrators: Full System: Full
%SystemRoot% \System32\ntbackup.exe	Administrators: Full System: Full
%SystemRoot% \system32\rcp.exe	Administrators: Full System: Full
%SystemRoot% \system32\reg.exe	Administrators: Full System: Full
%SystemRoot% \system32\regedt32.exe	Administrators: Full System: Full
%SystemRoot% \System32\regini.exe	Administrators: Full System: Full
%SystemRoot% \system32\regsvr32.exe	Administrators: Full System: Full
%SystemRoot% \system32\rexec.exe	Administrators: Full System: Full
%SystemRoot% \system32\route.exe	Administrators: Full System: Full
%SystemRoot% \system32\rsh.exe	Administrators: Full System: Full
%SystemRoot% \system32\sc.exe	Administrators: Full System: Full
%SystemRoot% \System32\secedit.exe	Administrators: Full System: Full
%SystemRoot% \system32\subst.exe	Administrators: Full System: Full
%SystemRoot% \System32\systeminfo.exe	Administrators: Full System: Full
%SystemRoot% \system32\telnet.exe	Administrators: Full System: Full
%SystemRoot% \system32\tftp.exe	Administrators: Full System: Full
%SystemRoot% \system32\tlntsvr.exe	Administrators: Full System: Full

The following registry ACLs will be configured for all environments.

Registry Permissions:

Object Name	Account Assignment	Permission
\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg	Administrators Backup Operators LOCAL SERVICE (*Exchange Enterprise Servers group on Domain Controllers and Exchange server* ***NOTE**: If permissions are sub-delegated with the Exchange Administration feature, then additional accounts and groups may appear on the Winreg key. If this has been done, then these should be documented with the site IAO and made available for any reviewer.*	all read(QENR) read(QENR) all

APPENDIX B. ADMINISTRATIVE TEMPLATE SETTINGS – MICROSOFT APPLICATIONS

In Windows 2003/XP/2000 additional controls can be set for Microsoft Applications using the Computer Administrative Templates and User Administrative Templates that are part of the system's Local Security Policy and are also configurable through Group Policy. The settings in this appendix are not yet referenced in the Windows 2003/XP/2000 Guides.

B.1 Terminal Services

Terminal Services are a new addition with Windows XP to the workstation line of Windows Operating Systems. Terminal Services will not be used on XP and additional settings are required to provide an additional level of security.

Terminal Services allow multiple users to connect from remote terminals and use the resources of the local machine as if they were physically at the machine. Terminal Services will not be used on servers that are not performing the role of Terminal Servers, or are not being used for Remote Administration.

B.1.1 Keep-Alive Messages

Keep-Alive messages are sent between the client and server to ensure that the connection state remains consistent with the client state. It is possible, in some situations, for a client to be physically disconnected from the network but for the session to remain open. If the client then reconnects, it could possibly create a new session but the original session could remain open. To prevent this from happening, Keep-Alive messages should be disabled.

- *(5.037: CAT III) The IAO will ensure that the setting, "Keep-Alive Messages" is set to "Disabled."*

B.1.2 Limit Users to One Remote Session

This setting limits users to one remote session. It is possible, if this setting is disabled, for users to establish multiple sessions.

- *(5.038: CAT II) The IAO will ensure that the setting, "Limit users to one remote session is set to "Enabled."*

B.1.3 Limit Number of Connections

This setting limits the number of simultaneous connections allowed to the terminal server. By default, unlimited connections are allowed. Allowing unlimited connections allows a potential denial of service (DoS) attack. The number of incoming connections should be limited.

- *(5.039: CAT II) The IAO will ensure that the setting, "Limit number of connections," is enabled and that the value of TS maximum connections allowed is no more than 1.*

NOTE: This number can be increased if the server is performing the role of a terminal server.

B.1.4 Do Not Use Temp Folders per Session

This setting, which is located under the Temporary Folders section of the Terminal Services configuration option, controls the use of per session temporary folders or of a communal temporary folder. If this setting is enabled, only one temporary folder is used for all terminal services sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

- *(5.044: CAT II) The IAO will ensure that the setting, "Do not use temp folders per session" is set to "Disabled."*

B.1.5 Do Not Delete Temp Folder upon Exit

This setting, which is located under the Temporary Folders section of the Terminal Services configuration option, controls the deletion of the temporary folders when the session is terminated. Temporary folders should always be deleted after a session is over to prevent hard disk clutter and potential leakage of information.

- *(5.045: CAT II) The IAO will ensure that the setting, "Do not delete temp folder upon exit" is set to "Disabled."*

B.1.6 Set Time Limit for Idle Sessions

This setting, which is located under the Sessions section of the Terminal Services configuration option, controls how long a session may be idle before it is automatically disconnected from the server. Users should disconnect if they plan on being away from their terminals for extended periods of time. Idle sessions should be disconnected after 15 minutes.

- *(5.047: CAT II) The IAO will ensure the setting, "Set time limit for idle sessions," is set to "Enabled" and the "Idle session limit" is set to no more than 15 minutes.*

B.1.7 Terminate Session When Time Limits are Reached

This setting, which is located under the Sessions section of the Terminal Services configuration option, controls whether or not clients are forcefully disconnected if their terminal services time limit is exceeded. If time limits are established for users, they should be enforced.

- *(5.049: CAT II) The IAO will ensure the setting, "Terminate session when time limits are reached," is set to "Enabled."*

B.2 Windows Installer

Windows Installer packages are structured packages being used for the distribution of software. Many new software products are using this distribution format, and the settings in this section control some of the installer's behavior.

B.2.1 Always Install with Elevated Privileges

If the Windows Installer is allowed to execute with elevated privileges, it can access areas of the system and perform actions that the account used to launch the installer may normally not have permission for. This could lead to unapproved software being installed or access to resources that the user cannot normally access.

- *(4.037: CAT I) The IAO will ensure that the setting, "Always install with elevated privileges" is set to "Disabled."*

B.2.2 Disable IE Security Prompt for Windows Installer Scripts

If this setting is enabled, users are not prompted when a web-based program attempts to install software on the system. Users should always be notified and asked for permission before a software package is installed to help prevent the installation of malicious software.

- *(5.050: CAT III) The IAO will ensure that the setting, "Disable IE security prompt for Windows Installer scripts" is set to "Disabled."*

B.2.3 Enable User Control Over Installs

This setting permits users to change installation settings that are normally only available to SAs. To do this, several Windows Installer security checks are bypassed. This setting should be disabled to prevent users from changing software installation options.

- *(5.051: CAT II) The IAO will ensure that the setting, "Enable user control over installs" is set to "Disabled."*

B.2.4 Enable User to Browse for Source While Elevated

This setting controls the ability of the user to browse the disk if an installer package executing with elevated privileges is executing. This could allow a user to access directories that they normally may not access.

- *(5.052: CAT II) The IAO will ensure that the setting, "Enable user to browse for source while elevated," is set to "Disabled."*

B.2.5 Enable User to Use Media Source While Elevated

This setting allows users to install programs from removable media when executing an installer package that is running with elevated privileges.

- *(5.053: CAT II) The IAO will ensure that the setting, "Enable user to use media source while elevated," is set to "Disabled."*

B.2.6 Enable User to Patch Elevated Products

This setting enables users to patch a product that was installed with elevated privileges. Such patching may result in the corruption or replacement of critical files and should not be allowed.

- *(5.054: CAT II) The IAO will ensure that the setting, "Enable user to patch elevated products," is set to "Disabled."*

B.2.7 Allow Admin to Install from Terminal Services Session

This setting allows Terminal Services Administrators to install and administer software remotely. Unless required for Remote Administration purposes, it should not be used.

- *(5.055: CAT II) Unless Terminal Services are being used for Remote Administration, the IAO will ensure that the setting, "Allow admin to install from Terminal Services session," is set to "Disabled."*

B.2.8 Cache Transforms in Secure Location on Workstation

Transforms are control files that specify many settings in customized installations of software packages that use the Windows installer. Normally a copy of the transform file is stored in the user's profile. The transform file may contain critical system information and should be stored in a secure location on the machine, instead of in a user's profile.

- *(5.056: CAT II) The IAO will ensure that the setting, "Cache transforms in secure location on workstation," is set to "Enabled."*

B.3 Windows Messenger

Windows Messenger is an instant messaging (IM) application created and distributed by Microsoft. There have been recent virus releases that use the Windows messenger client as a distribution method, since most virus scanners do not currently scan IM messages or files. In addition, IM clients require registration with a central server and may be the target of DoS or other attacks.

Windows Messenger also requires users to create a Microsoft Passport account in order to use the Instant Messenger applications on the Internet. Passport accounts are also created if a user signs up for an e-mail account on the Hotmail e-mail service. Several security vulnerabilities have been discovered recently in the Passport system that could lead to a compromise of the information stored on the passport servers.

Generally, Windows Messenger should not be active on a Windows 2003/XP/2000 system. However, if a site has a requirement for using Windows Messenger, then it will be permitted with the following conditions: All workstations and servers, with active Windows Messenger clients, should have personal firewalls installed that are configured to block access to public instant messaging providers such as AOL or MSN. The site must also have network controls in place to block the same access. Any applicable Microsoft security-related hot fixes must also be applied.

B.3.1 Do Not Automatically Start Windows Messenger Initially

This setting prevents the automatic launch of Windows Messenger at user logon.

- *(5.018: CAT II) If Windows Messenger has not been approved for use, the IAO will ensure that the setting "Do not automatically start Windows Messenger initially" is set to "Enabled."*

B.3.2 Prevent Windows Messenger from Accessing the Internet

The following Registry key should be created and configured to prevent Windows Messenger from accessing the MSN Messenger application on the Internet:

Registry Hive:	HKEY_LOCAL_MACHINE
Subkey:	\Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}
Value Name:	Disabled
Type:	REG_DWORD
Value:	1

- *(5.105: CAT II) If Windows Messenger is approved for use, the IAO will ensure that it has been configured to prevent access to the MSN Messenger Application.*

B.4 Logon

In general, it is good practice to ensure that all computer-related group policy changes are applied prior to users logging on so that the user can operate under the correct security context. Therefore, the following group policy setting is recommended:

- *(3.067: CAT II) The IAO will ensure that the setting "Always Wait for the Network at Computer Startup and Logon," is set to "Enabled."*

B.5 Group Policy

The Group Policy section contains several settings that control the refresh intervals and application rules that apply to group policy. The following setting ensures group policy settings are refreshed properly. If this setting is enabled, then Group Policy settings are not refreshed while a user is currently logged on. This could lead to instances when a user does not have the latest changes to a policy applied and is therefore operating in an insecure context.

- *(3.080: CAT II) The IAO will ensure that the setting, "Turn off background refresh of Group Policy" is set to "Disabled."*

B.6 Windows Time Service (Windows 2003/2000)

The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. The Windows Time Service attempts to synchronize with the Microsoft time server, time.windows.com. If the Windows Time Service is used, it should synchronize with a secure, authorized time source, and not the Microsoft time server.

- *(3.084: CAT III) The IAO will ensure that if the value for "Configure Windows NTP Client" is set to "Enabled," the "NtpServer" field points to an authorized time source.*

B.7 Network Connections

Settings under network connections control certain behavior when connected to a network.

B.7.1 Internet Connection Sharing

Internet connection sharing allows the computer to act as a gateway for other systems to access the Internet. It uses network address translation (NAT) to provide connections to multiple computers through a single Internet connection. This should not be used on a network as it could allow unauthorized machines access to the network.

- *(3.085: CAT II) The IAO will ensure that the setting, "Prohibit use of Internet Connection Sharing on your DNS domain network," is set to "Enabled."*

B.7.2 Network Bridge

A network bridge is used to connect various network segments to each other. Network bridges should be dedicated hardware, and other systems should not be used for this purpose.

- *(3.086: CAT II) The IAO will ensure that the setting, "Prohibit installation and configuration of Network Bridge on your DNS domain network," is set to "Enabled."*

B.8 Installation of Printers Using Kernel-mode Drivers

Kernel-mode drivers are drivers that operate in kernel mode. Kernel mode allows virtually unlimited access to hardware and memory. A poorly written kernel driver may cause system instability and data corruption. Malicious code inserted in a kernel-mode driver has almost no limit on what it may do. Most modern printers do not require kernel-mode drivers.

- *(3.087: CAT II) The IAO will ensure that the setting, "Disallow installation of printers using kernel-mode drivers," is set to "Enabled."*

B.9 Media Player – Automatic Downloads

The Windows Media Player uses software components, referred to as CODECs, to play back media files. By default, when an unknown file type is opened with the Media Player it will search the Internet for the appropriate CODEC and automatically download it. To ensure platform consistency and to protect against new vulnerabilities associated with media types, the SA must install all CODECs.

- *(5.061: CAT II) The IAO will ensure that the setting, "Prevent Codec Download," is set to "Enabled."*

The automatic check for updates performed by the Windows Media Player for XP must be disabled to ensure a constant platform and to prevent the introduction of unknown/untested software on the network. Creating the following registry key will prevent the Media Player from checking for automatic updates.

- *(5.060: CAT II) The IAO will ensure that the setting, "Prevent Automatic Updates," is set to "Enabled."*

This page is intentionally left blank.

APPENDIX C. APPLICATION SECURITY – OTHER APPLICATIONS

C.1 Internet Explorer Policy Settings

Internet Explorer, Microsoft's Web Browser, has been integrated with the Operating System to such an extent that it is essentially impossible to remove it from Windows. Although the option to remove the desktop and start menu icons is available, the underlying program is still there. Since it is impossible to remove, it should be configured as described in the *Desktop Application STIG* and the following settings should also be configured using the Administrative Templates section of the Local Computer Policy snap-in and through Group Policy. In addition all patches relating to Internet Explorer must be applied to the system.

C.1.1 Security Zones: Use Only Machine Settings

This setting enforces consistent security zone settings to all users of the computer. Security Zones control browser behavior at various web sites and it is desirable to maintain a consistent policy for all users of a machine.

- *(5.028: CAT II) The IAO will ensure that the setting, "Security Zones: Use only machine settings" is set to "Enabled."*

C.1.2 Security Zones: Do Not Allow Users to Change Policies

This setting prevents users from changing the Internet Explorer policies on the machine. Policy changes should be made by Administrators only, so this setting should be "Enabled."

- *(5.029: CAT II) The IAO will ensure that the setting "Security Zones: Do not allow users to change policies," is set to "Enabled."*

NOTE: This setting will make many of the security settings in Internet Explorer unavailable to the user.

C.1.3 Security Zones: Do Not Allow Users to Add/Delete Sites

This setting prevents users from adding sites to various security zones. Users should not be able to add sites to different zones, as this could allow them to bypass security controls of the system.

- *(5.030: CAT II) The IAO will ensure that the setting, "Security Zones: Do not allow users to add/delete sites" is set to "Enabled."*

C.1.4 Make Proxy Settings Per Machine (rather than per user)

This setting controls whether or not the Internet Explorer proxy settings are configured on a per-user or per-machine basis. All users of a machine should use the same proxy server to ensure consistent security policy enforcement.

- *(5.031: CAT II) The IAO will ensure that the setting, "Make proxy settings per-machine (rather than per user)," is set to "Enabled."*

C.1.5 Disable Automatic Install of Internet Explorer Components

This setting controls the ability of Internet Explorer to automatically install components if it goes to a site that requires components that are not currently installed. The SA should install all components on the system. If additional components are necessary, the user should inform the SA and have the SA install the components.

- *(5.032: CAT II) The IAO will ensure that the setting, "Disable Automatic Install of Internet Explorer components" is set to "Enabled."*

C.1.6 Disable Periodic Check for Internet Explorer Software Updates

This setting determines whether or not Internet Explorer will periodically check the Microsoft web sites to determine if there are updates to Internet Explorer available. The SA should manually install all updates on a system so that configuration control is maintained.

- *(5.033: CAT II) The IAO will ensure that the setting, "Disable Periodic Check for Internet Explorer software updates" is set to "Enabled."*

C.1.7 Disable Software Update Shell Notifications on Program Launch

Microsoft Internet Explorer now supports a software distribution channel that may be used to update software installed on a machine. If this setting is enabled, users will not be notified when programs are modified through the software distribution channel. A user should always be notified when a software package is updated so that unauthorized or suspicious updates may be reported.

- *(5.034: CAT II) The IAO will ensure that the setting, "Disable software update shell notifications on program launch" is set to "Disabled."*

APPENDIX D. RELATED PUBLICATIONS

Government Publications

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 2003.

Department of Defense (DOD) Directive 8500.1, "Information Assurance," October 2002.

Department of Defense (DOD) Instruction 8500.2, "Information Assurance (IA) Implementation," February 2003.

Defense Information Systems Agency (DISA)/Chief Information Officer, Memorandum for Distribution, "DISA Standard Computer Configurations," Version 1999-A, November 1998.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency (DISA)/Defense Information Services Organization (DISO) Naming Convention Standards, March 1994.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Active Directory," Version 1.0, December 2000.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Group Policy," Version 1.1, September 2001.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 File and Disk Resources," Version 1.0, 19 April 2001.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," Version 1.2, December 2002.

National Security Agency (NSA), "Guide to Securing Microsoft Windows NT Networks," Version 4.2, 18 September 2001.

National Security Agency (NSA), "Guide to Securing Microsoft Windows XP," Version 1.1, 1 December 2003.

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 October 1991.

Army Regulation (AR) 25-2, "Information Assurance," 14 November 2003.

Air Force Instruction (AFI) 33-202, "Computer Security."

Air Force Systems Security Memorandum (AFSSI) 5002, “Control/Access Protection,” 25 March 1991.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, “Department of the Navy Automated Information Systems (AIS) Security Program,” 15 November 1989.

Navy Staff Office Publication (NAVSO Pub) 5239-15, “Controlled Access Protection Guidebook,” August 1992.

General Accounting Office Report to Congressional Requester (GAO/AIMD-96-84), “Information Security Computer Attacks at Department of Defense Pose Increasing Risks.”

Field Security Operations Publications

DISA Computing Services Security Handbook, Version 3, 1 December 2000

DISA Database Security Technical Implementation Guide (STIG)

DISA Desktop Application Security Technical Implementation Guide (STIG)

DISA Enclave Security Technical Implementation Guide (STIG)

DISA Network Infrastructure Security Technical Implementation Guide (STIG)

Commercial and Other Publications

Microsoft Solutions for Security, Windows 2003 Security Guide, 2003

Microsoft Solutions for Security, Threats and Countermeasures: Security Settings in Windows 2003 and Windows XP, 2003

Microsoft Windows 2003 and XP Specialized Security – Limited Functionality Templates (To be published)

Microsoft Windows XP Security Guide v2.0, 2004

Web Sites

DISA	http://www.disa.mil
DISA Datahouse	https://datahouse.disa.mil
DISA Field Security Operations	https://guides.ritchie.disa.mil
DISA Information Assurance	https://iase.disa.mil
DOD-JTF-GNO	http://www.cert.mil
Mergent (encryption software)	http://www.mergent.com
Microsoft's Knowledge Base Web Site	http://www.microsoft.com/kb/
NCSA	http://www.ncsa.com
Netscape	http://wp.netscape.com/security/index.html
RSA Data Systems (encryption software)	http://www.rsa.com
Symantec Corporation (ESM)	http://www.symantec.com
Vulnerability Compliance Tracking System (VCTS)	https://vms.disa.mil

This page is intentionally left blank.

APPENDIX E. LIST OF ACRONYMS

ACL	Access Control List
ADS	Audit Alternate Data Streams
AIS	Automated Information System
AS	Authentication Server
CCB	Configuration Control Board
CD	Compact Disk
CIS	The Center for Internet Security
CMOS	Complementary Metal-Oxide Semiconductor
COTS	Commercial Off-The-Shelf
DAA	Designated Approving Authority
DECC	Defense Enterprise Computer Center
DECC-D	Defense Enterprise Computer Center - Detachment
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DLL	Dynamic Link Library
DNS	Domain Name Server
DOD	Department of Defense
DOD JTF-GNO	Department of Defense Computer Emergency Response Team
DoS	Denial of Service
FTP	File Transfer Protocol
GAO	General Accounting Office
GOTS	Government-Off-The-Shelf
HPFS	High Performance File System
HTTP	Hyper Text Transport Protocol
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAW	In Accordance With
IE	Internet Explorer
IETF	Internet Engineering Task Force
IG	Inspector General
IIS	Internet Information Server
INFOSEC	Information Security
INFOWAR	Information Warfare
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IS	Information System
ITA	Intruder Alert
JID	Joint Intrusion Detector
JPEG	Joint Photographic Experts Group

JTF-GNO	Joint Task Force – Global Network Operations
LAN	Local Area Network
LM	LanManager
LSA	Local Security Authority
MAPI	Mail Application Programming Interface
MD5	Message Digest Version 5
MMC	Microsoft Management Console
MOA	Memorandum of Agreement
NCSC	National Computer Security Center
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NID	Network Intrusion Detector
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NNTP	Network News Transfer Protocol
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSO	Network Security Officer
NTFS	NT File System
OS	Operating System
PC	Personal Computer
PCT	Private Communications Technology
PDC	Primary Domain Controller
POC	Point-of-Contact
POP	Point-of-Presence
POSIX	Portable Operating System Interface for Computing Environments
PPE	Password Policy Enforcer
PPP	Point-to-Point Protocol
RAM	Random Access Memory
RAS	Remote Access Service
RCC	Regional Control Center
RCERT	Regional CERT
RISC	Reduced Instruction Set Computer
RNOSC	Regional Network Operations and Security Center
RPC	Remote Procedure Call
RSA	Regional Support Activity
RSC	Regional Service Center
SA	System Administrator
SAM	Security Accounts Manager
SBU	Sensitive but Unclassified
SCSI	Small Computer Systems Interface
SID	Security Identifier

SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SRM	Security Reference Monitor
SRR	Secure Readiness Review
SSL	Secure Sockets Layer
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TAPI	Telephony Applications Programming Interface
TASO	Terminal Area Security Officer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator
VAAP	Vulnerability Analysis and Assistance Program
VCTS	Vulnerability Compliance Tracking System
VGA	Video Graphics Array
VMS	Vulnerability Management System
WAN	Wide Area Network
WINS	Windows Internet Name Service
WWW	World Wide Web

This page is intentionally left blank.